

Exam : SY0-701

Title : CompTIA Security+

<https://www.passcert.com/SY0-701.html>

1.A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

- A. Serverless framework
- B. Type 1 hypervisor
- C. SD-WAN
- D. SDN

Answer: A

Explanation:

A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.

A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.

SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.

SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 264-265; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00; [Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

2.A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

- A. The user jsmith's account has been locked out.
- B. A keylogger is installed on [smith's workstation
- C. An attacker is attempting to brute force ismith's account.
- D. Ransomware has been deployed in the domain.

Answer: C

Explanation:

Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident.

References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes – SY0-601 CompTIA Security+ : 1.1

3.Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

- A. Jailbreaking
- B. Memory injection
- C. Resource reuse
- D. Side loading

Answer: D

Explanation:

Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices.

References = Sideloaded - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers – CompTIA Security+ SY0-501 – 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

4.A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors.

Which of the following should the systems administrator use?

- A. Packet captures
- B. Vulnerability scans
- C. Metadata
- D. Dashboard

Answer: D

Explanation:

A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria¹².

A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors¹³.

A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter¹⁴.

Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards – SY0-601 CompTIA Security+ : 4.3, video by Professor Messer³: CompTIA Security+ SY0-701

Certification Study Guide, page 3464:

CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

5.A technician needs to apply a high-priority patch to a production system.

Which of the following steps should be taken first?

- A. Air gap the system.
- B. Move the system to a different network segment.
- C. Create a change control request.
- D. Apply the patch to the system.

Answer: C

Explanation:

= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches.

References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.

6.Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

- A. SCAP

- B. Net Flow
- C. Antivirus
- D. DLP

Answer: D

Explanation:

DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets.

References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5, page 11.

7.A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

- A. Local data protection regulations
- B. Risks from hackers residing in other countries
- C. Impacts to existing contractual obligations
- D. Time zone differences in log correlation

Answer: A

Explanation:

Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders. Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States. A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage. Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there.

References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269. CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

8.A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work.

Which of the following is the best option?

- A. Send out periodic security reminders.
- B. Update the content of new hire documentation.
- C. Modify the content of recurring training.
- D. Implement a phishing campaign

Answer: C

Explanation:

Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can cover the latest threats, best practices, and policies that are relevant to their work environment. Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles.

References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

9. A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks.

SIEM alerts have not yet been configured.

Which of the following best describes what the security analyst should do to identify this behavior?

- A. [Digital forensics
- B. E-discovery
- C. Incident response
- D. Threat hunting

Answer: D

Explanation:

Threat hunting is the process of proactively searching for signs of malicious activity or compromise in a network, rather than waiting for alerts or indicators of compromise (IOCs) to appear. Threat hunting can help identify new tactics, techniques, and procedures (TTPs) used by malicious actors, as well as uncover hidden or stealthy threats that may have evaded detection by security tools. Threat hunting requires a combination of skills, tools, and methodologies, such as hypothesis generation, data collection and analysis, threat intelligence, and incident response. Threat hunting can also help improve the security posture of an organization by providing feedback and recommendations for security improvements.

References = CompTIA Security+ Certification Exam Objectives, Domain 4.1: Given a scenario, analyze potential indicators of malicious activity. CompTIA Security+ Study Guide (SY0-701), Chapter 4: Threat Detection and Response, page 153. Threat Hunting – SY0-701 CompTIA Security+ : 4.1, Video 3:18. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 3.

10. A systems administrator works for a local hospital and needs to ensure patient data is protected and secure.

Which of the following data classifications should be used to secure patient data?

- A. Private
- B. Critical
- C. Sensitive
- D. Public

Answer: C